



Government
Property
Agency

GPA Data Privacy Notice

Published 9 October 2026

DOCUMENT CLASSIFICATION: OFFICIAL

Summary

This privacy notice informs you of how the Government Property Agency (GPA) looks after your personal data, your privacy rights, and how to exercise them under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Your personal data is stored securely at all times within our secure Property and Workplace systems. Only authorised individuals who have a genuine business or legal need can access your information.

To provide an effective government estate, we may share information about you with other Government Departments, Arms-Length Bodies, and our authorised service providers (such as facilities management and security partners) who are directly involved in delivering your workplace services. Your data will not be shared with anyone not listed in this notice unless we are legally obliged to do so.

Where we conduct User Research or Customer Insight to improve our buildings, we will only use your identifiable information with your explicit consent, which you can withdraw at any time.

A full list of the systems we use and the organisations we share information with is provided in the later sections of this Privacy notice.

Who we are and how to contact us

The Government Property Agency (GPA) is an executive agency of the Cabinet Office. We are responsible for providing government departments and arms-length bodies with excellent places to work for their civil servants, which in turn enables them to deliver high-quality public services. We act as the central body responsible for the strategic management of government offices, ensuring that workplace solutions are safe, efficient, and technology-enabled.

For most day-to-day property and workplace functions, the GPA is the controller. However, for specific corporate functions (such as HR and high-level commercial activity), the Cabinet Office may act as the controller.

If you have any questions about this privacy notice or how we handle your data, please contact our Data Protection Team:

- **Email:** dataprotection@gpa.gov.uk
- **Post:** GPA Data Protection Team, 23 Stephenson Street, Birmingham, B2 4BH

Our Data Protection Officer (DPO) can be contacted at: dpo@cabinetoffice.gov.uk.

The personal data we collect

At the GPA, we process the following categories of personal information about our clients, staff, and building occupants to deliver our services:

- **Identity & Contact Information:** Full name, employer, department (MD code), job title, email address, phone number, and unique identifiers (Staff, Contractor, or Supplier IDs).
- **Security and Access data:** Security clearance/vetting status, site access permissions, photographs for ID passes (**GovPass**), and building entry/exit logs..
- **Visual and Digital data:** CCTV images for safety and security, IP/MAC addresses (for GPA WiFi usage), and occupancy data.
- **Workplace Usage data:** Room and desk booking history (Matrix), printing logs (GovPrint), and helpdesk/service request records (ServiceNow/Planon).
- **Special Category data:** Health-related data (limited to Health and Safety or emergency response needs, such as PEEPs) or protected characteristics used for anonymised diversity monitoring in user research (with explicit consent).
- **Aggregated data:** A combination of usage and occupancy data used for business intelligence and estate planning to enable us to predict future space requirements. Individuals cannot be identified from this data.

DOCUMENT CLASSIFICATION: OFFICIAL

Why we collect personal data

We use personal data to carry out our functions as an executive agency and to ensure we process your data fairly and transparently, we categorise our activities into Direct Service Delivery, Estate Planning, and Statutory Obligations.

Direct Service Delivery and Administration

We process your personal information to provide the essential daily services you use within the government estate. This includes:

- **Building Access & Security:** Identifying you at the point of entry and ensuring you have the correct security clearance to access specific sites or secure zones (e.g., **GovPass**).
- **Workplace Bookings:** Managing your reservations for desks, lockers, and meeting rooms (e.g., **Matrix**).
- **Property Technology:** Providing you with shared infrastructure, including secure **WiFi**, **GovPrint** services, and audio-visual equipment.
- **Safety & Helpdesk:** Responding to your facilities requests or emergency incidents via our helpdesk (e.g., **ServiceNow/Planon**).

Estate Planning and Research (Secondary Uses)

We also process information for broader purposes to ensure the government estate is efficient and cost-effective. These include:

- **Occupancy Monitoring:** Using anonymised data to understand how buildings are used, allowing us to manage capacity and plan for future office requirements.
- **User Research & Surveys:** Contacting you (with your consent) to participate in research panels or surveys (e.g., **Leesman**, **Spoonfed**, or **Amnesty Survey**) to improve building design and customer experience.
- **Financial Management:** Managing property transactions, rental agreements, and billing for the departments and bodies occupying our buildings.
- **System Testing & Development:** Occasionally using data in secure test environments to improve our digital platforms (e.g., **Business Central Finance Copilot** or **Salesforce** updates).

Statutory Disclosures

DOCUMENT CLASSIFICATION: OFFICIAL



In specific circumstances, we may be required by law to share your information without your direct consent. This includes:

- **Public Safety:** Sharing **CCTV footage** or access logs with law enforcement for the prevention or detection of crime.
- **Public Inquiry/Audit:** Providing data for statutory audits (**National Audit Office**) or independent investigations where there is a legal requirement to do so.

Lawful basis for processing

Under the UK GDPR, the GPA relies on several lawful bases to process personal data depending on the context of the service being provided:

- **Public Task (Article 6(1)(e)):** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority. This is our primary basis for managing the government estate, providing workplace functions, and operating CCTV for the safety and security of building occupants and property.
- **Performance of a Contract (Article 6(1)(b)):** Processing is necessary for managing supplier relationships, commercial activities, and property transactions.
- **Legal Obligation (Article 6(1)(c)):** Processing is necessary for compliance with our legal duties, including security vetting, health & safety reporting (such as RIDDOR), and statutory financial reporting.
- **Vital Interests (Article 6(1)(d)):** Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- **Special Category Data (Article 9):** We process sensitive data (such as health data for emergency evacuation plans) under the basis of Substantial Public Interest (statutory functions) or **Health & Social Care** obligations.

Who we share your personal data with

We use several commercial companies and strategic partners to either store personal information or to manage it on our behalf, and to provide certain services to you. Where we have these arrangements, there is always a contract, a Memorandum of Understanding (MoU), or an Information Sharing Protocol in place to ensure that the organisation complies with data protection law.

We may share personal data with:

DOCUMENT CLASSIFICATION: OFFICIAL



- **Other Government Departments (OGDs) and agencies:** Including HM Treasury and HMRC. Specifically via **GovPass** to enable cross-government "roaming" and building access.
- **Local authorities and arm's-length bodies:** To facilitate regional estate management.
- **Audit Bodies:** The National Audit Office (NAO) and the Government Internal Audit Agency (GIAA) for audit and transparency purposes.
- **Legal Counsel:** The Government Legal Department (GLD) and external legal counsel.
- **Law Enforcement:** Bodies such as the Police, where we are obliged to do so by law.
- **Strategic Partners and Independent Suppliers:** Providing services such as facilities management, catering, security, and IT support.
- **Emergency Services:** Providing services to protect the vital interests of others by processing one individual's personal data.

We may also share your personal information when there is a pressing and legal reason that outweighs your right to confidentiality, such as for the detection and prevention of crime or to protect individuals at serious risk of harm. All data sharing is lawful and proportionate, covered by contracts or agreements, and subject to appropriate security and confidentiality controls. We **do not** provide personal information to any other organisation for direct marketing.

International Transfers

While the GPA prioritises UK and EEA-based storage (e.g., Azure regions in Ireland and the Netherlands), technical support for some systems (such as catering management) is provided by staff in the United States.

Where data is accessed from outside the UK/EEA, we ensure equivalent protection through:

- UK Adequacy Regulations (e.g., the UK-US Data Bridge).
- Appropriate Safeguards (such as the UK International Data Transfer Addendum).
- Transfer Risk Assessments (TRAs) to validate security controls.

How we keep your personal data secure

We take the security of your data very seriously. We have implemented robust technical and organisational measures to prevent your personal data from being accidentally lost, used, or accessed in an unauthorised way.

- **Encryption:** Data is encrypted at rest and in transit using industry-standard protocols.
- **Access Control:** We use Role-Based Access Control (RBAC), meaning only authorised staff with a specific business need can view your information.
- **Auditing:** Our systems are subject to regular Independent Technical Health Checks (ITHC) to identify and fix vulnerabilities.
- **Staff Training:** All GPA staff and relevant contractors undergo mandatory Data Protection and Security training annually.

How long we keep your data (Retention)

Personal data is retained only for as long as necessary for its purpose. Retention periods are defined in the Records Management Procedure and Retention Schedules and takes account of legal, regulatory, and business needs.

The GPA maintains specific retention periods for different categories of information. For further information regarding specific timeframes, please contact the Data Protection Team at dataprotection@gpa.gov.uk

In limited circumstances, the GPA may retain information beyond its standard retention period for archiving, research or strategic planning purposes where this supports the delivery of public services. In such cases, the data will be anonymised or otherwise protected so that individuals can no longer be identified.

Your Data Protection Rights

Under the Data Protection Act 2018 and UK GDPR, you have several rights regarding your personal information. These include:

- **The right to be informed:** This privacy notice fulfills our obligation to tell you how we use your data.
- **The right of access:** You can ask for a copy of the personal information we hold about you.
- **The right to rectification:** You can ask us to correct information you think is inaccurate or complete information you think is incomplete.

DOCUMENT CLASSIFICATION: OFFICIAL



- **Right to erasure (Right to be forgotten):** The right to ask us to erase your personal information in certain circumstances.
- **The right to restrict processing:** You can ask us to limit how we use your data in certain circumstances.

Please note that some rights may be limited or may not apply where we are required to process personal data to perform a public task, comply with legal obligations or protect the rights and freedoms of others. Where a limitation applies, we will explain this to you when responding to your request.

To exercise any of your data subject rights, including a request for copies, deletion, or correction of your data, please contact the GPA Data Protection Team:

GPA Data Protection Team

Government Property Agency
23 Stephenson Street Birmingham,
B2 4BH

Email: dataprotection@gpa.gov.uk

In circumstances where you request deletion or correction and we have shared your personal information with third parties (such as strategic partners or other government departments), we will take reasonable steps to ensure they also update or delete the information in line with your request.

In addition to this general Privacy Notice, we encourage you to review our specific privacy notices relevant to particular services to understand the unique processing activities involved.

How to complain

If you consider your data has been mishandled, please contact our Data Protection Team at dataprotection@gpa.gov.uk. You can also contact the DPO dpo@cabinetoffice.gov.uk

If you remain dissatisfied with the outcome of your complaint, you can refer the matter for adjudication to the [Information Commissioner's Office \(ICO\)](#) via their website or by using the contact details below.

Information Commissioner's Office,

DOCUMENT CLASSIFICATION: OFFICIAL



Wycliffe House, Water Lane,
Wilmslow, Cheshire, SK9 5AF
Telephone: 0303 123 1113
Email: casework@ico.org.uk

Future changes

This Privacy Notice is reviewed regularly to ensure it remains accurate, transparent and compliant with evolving data protection legislation and regulatory guidance.

Version:

Date: April 2026

Next Review date: April 2027

DOCUMENT CLASSIFICATION: OFFICIAL